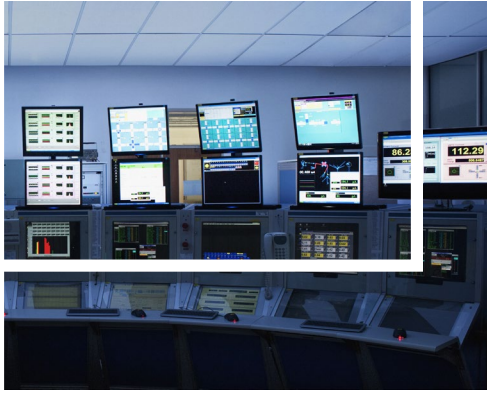
次世代のITインフラ - ゼロトラスト・アーキテクチャ
ITインフラの役割変化とゼロトラストの適合性



PwCコンサルティング合同会社　シニアマネージャー　神野 光祐

1.IT利活用の変化に、インフラは追随できているか

デジタルトランスフォーメーション（DX）の必要性が叫ばれて久しい昨今、ITの技術的な側面だけでなく、ビジネスにおけるユースケースの進化・高度化が続いています。もはや「ITはIT部門が担当するもの」という考え方も薄れつつあり、「Shadow IT（IT統括部門の把握・管理外におけるデバイスやクラウドサービスの利用）」の問題顕在化が示すように、ビジネス部門も自由闊達にITを利用するようになりました。

一方でITインフラは、このような変化に追随しているのでしょうか。実態として、多くの企業ではEoL（End of Life）対応のリプレイスやセキュリティ機能の追加などは行っているものの、「ITインフラアーキテクチャの見直し」を行っているケースは少ないのではないでしょうか。

本稿では、昨今特に注目を浴びている「ゼロトラスト・アーキテクチャ」の考え方に基づくITインフラアーキテクチャの見直しを見据え、

- 今日におけるITやそのユースケースがもたらす、ITインフラへの要求変化
- ITインフラへの要求に対するゼロトラスト・アーキテクチャの適合性

について触れ、自社のITインフラをゼロトラスト化する意義を中心に解説していきます。

2.ITインフラへの要求に変化をもたらす要素

ITインフラに要求されることを考えるために、まずは企業を取り巻く状況を見ていきましょう。

- ビジネスのデジタル化およびアジリティ向上

今やDXを意識しない企業はないと言ってよいほど、デジタル化の波はビジネスに大きな影響を及ぼしています。DXは、単にビジネスにITを組み込むことに留まりません。業種・業態の境界線を越えてスピーディにビジネスを展開するために、ビジネスとITを密に組み合わせ、アジャイルにシステムを構築する動きにつながっています。これにより、社内のIT部門のみならずビジネス部門、さらには社外の関係者がタッグを組むなど、1つのIT環境の中に多様な人物が入り混じる構図が生まれています。

また、上記と関連したクラウドサービスの利用拡大も無視できません。クラウドサービスは、IT利活用ひいてはビジネス自体のアジリティ向上に寄与しますが、一方でコンプライアンスとセキュリティにおけるリスクを浮き彫りにもしています。

- 働き方改革・リモートワーク定着の潮流

新型コロナウイルス感染症（COVID-19）により、多くの企業では在宅勤務（リモートワーク）へのシフトが行われました。では、この「リモート化」の潮流は、いわば一過性のBCP（Business Continuity Plan：事業継続計画）対応として、事の収束と共に縮小していくのでしょうか。私たちはまた、これまでと同じようにオフィスに出社して仕事をするようになるのでしょうか。

今回の潮流によって、「出社しなくても十分に仕事ができる」と気付く従業員が一定数いるものと考えられますし、従来から子育て・介護などを筆頭に「出社しないワークスタイルが望ましい」層もいます。リモートワーク制度の整備・浸透度合いが、人材獲得ひいては競争力の源泉となるシナリオも十分現実的でしょう。

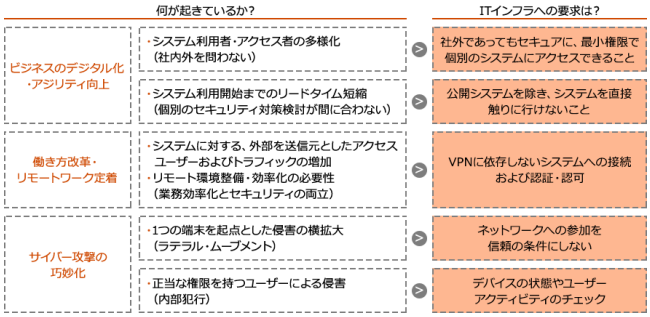
■ サイバー攻撃の巧妙化

多くの企業は、エンドポイントセキュリティおよびネットワークセキュリティを筆頭に、種々のセキュリティ対策を打っています。一方、そのような企業であっても、残念ながら被害に遭ってしまうケースが後を絶ちません。

認証された端末が侵害を受け、それがネットワークを通じて他のシステムに波及する、もしくは認証されたユーザーが意図的な不正を働くケースなど、セキュリティ対策でカバーし切れない「抜け穴」を突かれるケースも枚挙にいとまがありません。

上記の要素を勘案すると、ITインフラには「インフラたる安定性や安全性」を維持しつつ、より高度な認証・認可の機能、ならびにビジネスに対応するアジリティが要求されていると言えます（図表1）。

図表1：企業を取り巻く状況とITインフラへの要求

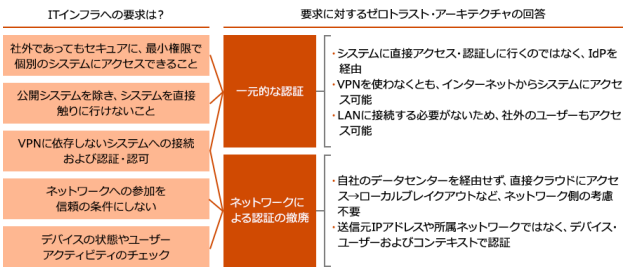


3.ITインフラへの要求に応えるゼロトラスト・アーキテクチャ

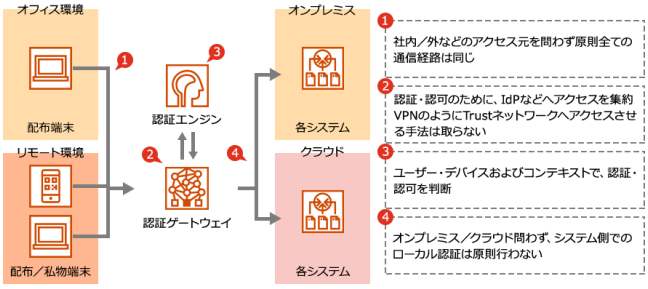
こうした複雑かつ広範な対応を求められる現代において、注目されるセキュリティの概念がゼロトラスト・アーキテクチャです。ゼロトラスト・アーキテクチャは、その名の通り「信頼しない」こと、つまり「毎回認証・検証すること」を基本的な考え方としています。端末の接続ネットワークが社内LANであろうとインターネットであろうと、手放しで信頼することはありません。裏を返せば、社内LANに接続されていないユーザーやデバイス（社外の関係者やリモートワーカー）であっても、同様の安全性を担保することが可能になるわけです。これは、接続元ネットワークを問わず、統合的にユーザーやデバイスおよびコンテキストに基づき認証・認可を行うことで実現されます（図表2）。

この考え方は、上述したITインフラへの要求の変化にも合致する内容です。ゼロトラスト化により、安定的・安全かつ柔軟なITインフラを実現可能です（図表3）。

図表3：ゼロトラスト・アーキテクチャの特徴



図表2：ゼロトラスト・アーキテクチャの概要



ここまで読む限り、「ゼロトラスト・アーキテクチャはよいこと尽くしである」と思われるかもしれません。では、全ての企業は、すぐにゼロトラスト・アーキテクチャの導入に着手すべきなのでしょうか。次稿では、ゼロトラスト・アーキテクチャ導入に際して押さえておくべきポイントを紹介します。

お問い合わせ

PwCコンサルティング合同会社
〒100-6921　東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel：03-6250-1200（代表）　Mail：jp_cyber_inquiry@pwc.com